

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-254807

(43) 公開日 平成10年(1998) 9月25日

(51) Int.Cl. <sup>4</sup>	識別記号	F I	
G 0 6 F 13/00	3 5 5	G 0 6 F 13/00	3 5 5
	3 5 1		3 5 1 G
15/00	3 1 0	15/00	3 1 0 E
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A
12/56			6 7 5 B

審査請求 未請求 請求項の数55 OL (全 18 頁) 最終頁に続く

(21) 出願番号 特願平10-10779

(22) 出願日 平成10年(1998) 1月22日

(31) 優先権主張番号 08/787557

(32) 優先日 1997年1月22日

(33) 優先権主張国 米国 (US)

(71) 出願人 596077259

ルーセント テクノロジーズ インコーポ  
レイテッドLucent Technologies  
Inc.アメリカ合衆国 07974 ニュージャージ  
ー、マレーヒル、マウンテン アベニュー  
600-700

(72) 発明者 エラン ガバー

アメリカ合衆国、07901 ニュージャージ  
ー、サミット、ニュー イングランド ア  
ベニュー 15ビー

(74) 代理人 弁理士 三保 弘文

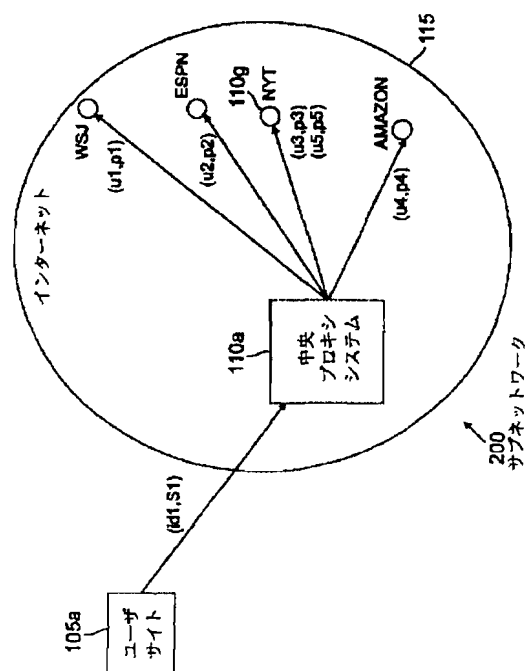
最終頁に続く

(54) 【発明の名称】 匿名的にサーバサイトを閲覧する方法

(57) 【要約】

【課題】 ユーザの秘密性を保ちながらユーザの識別を提供する、匿名性のある個人化されたウェブ閲覧を行う。

【解決手段】 本発明は、ユーザサイト105aと、ユーザサイト105aによって閲覧されることが可能サーバサイト110gとを有するネットワーク200で使用する。中央プロキシシステム110aは、(1)ユーザサイト105aに固有のデータから生成されるサイト固有の代用識別子を処理する第1ルーチンと、(2)代用識別子をサーバサイト110gへ送信した後、ユーザサイト105aから受信される閲覧コマンドをサーバサイト110gへ再送する第2ルーチンと、(3)閲覧コマンドのうちユーザサイト105aの識別をサーバサイト110gに明らかにする部分を除去(および置換)する第3ルーチンを有する。



## 【特許請求の範囲】

【請求項1】 ネットワークに接続され、ユーザが中央プロキシシステムを通じて匿名的に前記ネットワーク上のサーバサイトを閲覧することを可能にする中央プロキシシステムにおいて、

前記ユーザに固有のデータから生成されるサイト固有の代用識別子を処理するコンピュータ実行可能な第1ルーチンと、

前記代用識別子を前記サーバサイトへ送信した後、前記ユーザから受信される閲覧コマンドを前記サーバサイトへ再送するコンピュータ実行可能な第2ルーチンと、  
前記閲覧コマンドのうち前記ユーザの識別を前記サーバサイトに明らかにする部分を除去するコンピュータ実行可能な第3ルーチンとからなることを特徴とする中央プロキシシステム。

【請求項2】 前記データは、前記ユーザによって供給される識別データおよびユーザ定義可能文字列からなることを特徴とする請求項1の中央プロキシシステム。

【請求項3】 前記サイト固有の代用識別子は、サイト固有の代用ユーザ名およびサイト固有の代用ユーザパスワードからなることを特徴とする請求項1の中央プロキシシステム。

【請求項4】 前記第1ルーチンは、前記データから前記ユーザに対するサイト固有の代用電子メールアドレスを生成することを特徴とする請求項1の中央プロキシシステム。

【請求項5】 前記第1ルーチンは、前記サーバサイトのアドレスから前記サイト固有の代用識別子を生成することを特徴とする請求項1の中央プロキシシステム。

【請求項6】 前記サーバサイトは、前記ユーザにウェブページを提示することが可能なワールドワイドウェブサイトであり、前記第2ルーチンは、前記ユーザの指示の下で前記代用識別子を前記サーバサイトへ送信することを特徴とする請求項1の中央プロキシシステム。

【請求項7】 前記第2ルーチンは、前記ユーザによってウェブページフィールドに供給される英数字コードに基づいて前記代用識別子を前記サーバサイトへ送信することを特徴とする請求項1の中央プロキシシステム。

【請求項8】 前記英数字コードはエスケープシーケンスとして構成されることを特徴とする請求項7の中央プロキシシステム。

【請求項9】 前記ユーザは前記ウェブページフィールドに前記英数字コードを手入力することを特徴とする請求項7の中央プロキシシステム。

【請求項10】 前記中央プロキシシステムは、前記ユーザに付随するコンピュータ実行可能なローカルルーチンと通信し、該ローカルルーチンは、前記ユーザに固有のデータから前記サイト固有の代用識別子を生成することを特徴とする請求項9の中央プロキシシステム。

【請求項11】 前記ユーザ宛の電子メールを格納する

ことが可能なデータ記憶領域をさらに有することを特徴とする請求項1の中央プロキシシステム。

【請求項12】 前記第1ルーチンは、前記ユーザから受信されるデータに擬似ランダム関数およびハッシュ関数を適用することによって構成される代用識別子を処理することを特徴とする請求項1の中央プロキシシステム。

【請求項13】 前記ユーザごとに、前記サーバサイトに固有の電子メールボックスを格納することが可能なデータ記憶領域をさらに有することを特徴とする請求項1の中央プロキシシステム。

【請求項14】 各電子メールボックスは付随する鍵を有し、該鍵は前記データとインデックス番号の関数であることを特徴とする請求項13の中央プロキシシステム。

【請求項15】 与えられた代用識別子に対して、複数のサイト固有電子メールボックスに格納された前記ユーザ宛の電子メールを収集するコンピュータ実行可能なルーチンをさらに有することを特徴とする請求項1の中央プロキシシステム。

【請求項16】 前記第1ルーチンは、前記閲覧コマンドに付加されたセッションタグを受信し、前記中央プロキシシステムは、該セッションタグを使用して、前記代用識別子を各閲覧コマンドと関連づけることを特徴とする請求項1の中央プロキシシステム。

【請求項17】 前記サーバサイトがアクセス可能な、前記ユーザに固有のセッション情報を格納することが可能なデータ記憶領域をさらに有することを特徴とする請求項1の中央プロキシシステム。

【請求項18】 電子支払い情報を格納することが可能なデータ記憶領域をさらに有し、前記ユーザは該電子支払い情報を使用して前記サーバサイトとの匿名商取引を行うことを特徴とする請求項1の中央プロキシシステム。

【請求項19】 前記ユーザに固有のデータから前記サイト固有の代用識別子を生成し該サイト固有の代用識別子を前記第1ルーチンへ送信する初期化ルーチンをさらに有することを特徴とする請求項1の中央プロキシシステム。

【請求項20】 ネットワークに接続され、少なくとも1つのユーザが中央プロキシシステムを通じて匿名的に前記ネットワーク上のサーバサイトを閲覧することを可能にする周辺プロキシシステムにおいて、該周辺プロキシシステムは、

特定ユーザから受信されるデータから特定代用識別子を生成するコンピュータ実行可能な第1ルーチンと、  
前記特定代用識別子を前記中央プロキシシステムへ送信するコンピュータ実行可能な第2ルーチンとからなり、  
前記中央プロキシシステムは、前記特定代用識別子を前記サーバサイトへ再送した後、前記特定ユーザから受信

される閲覧コマンドを前記サーバサイトへ再送することを特徴とする周辺プロキシシステム。

【請求項21】 前記データは、前記特定ユーザによって供給される識別データおよびユーザ定義可能文字列からなることを特徴とする請求項20の周辺プロキシシステム。

【請求項22】 前記特定代用識別子は、特定代用ユーザ名および特定代用ユーザパスワードからなることを特徴とする請求項20の周辺プロキシシステム。

【請求項23】 前記第1ルーチンは、前記データから前記特定ユーザに対する特定代用電子メールアドレスを生成することを特徴とする請求項20の周辺プロキシシステム。

【請求項24】 前記第1ルーチンは、前記サーバサイトのアドレスから前記特定代用識別子を生成することにより、前記特定代用識別子は前記サーバサイトに固有なものとなることを特徴とする請求項20の周辺プロキシシステム。

【請求項25】 前記サーバサイトは、前記ユーザに少なくとも1つのウェブページを提示することが可能なワールドワイドウェブサイトであり、前記中央プロキシシステムは、前記特定ユーザの指示の下で前記特定代用識別子を前記サーバサイトへ送信することを特徴とする請求項20の周辺プロキシシステム。

【請求項26】 前記中央プロキシシステムは、前記特定ユーザによってウェブページフィールドに供給される英数字コードに基づいて前記特定代用識別子を前記サーバサイトへ送信することを特徴とする請求項20の周辺プロキシシステム。

【請求項27】 前記英数字コードはエスケープシーケンスとして構成されることを特徴とする請求項26の周辺プロキシシステム。

【請求項28】 前記中央プロキシシステムは、前記閲覧コマンドのうち前記特定ユーザの識別を前記サーバサイトに明らかにする部分を除去するコンピュータ実行可能な第3ルーチンをさらに有することを特徴とする請求項20の周辺プロキシシステム。

【請求項29】 前記第1および第2ルーチンは前記特定ユーザに付随するコンピュータシステム上で実行可能であり、前記中央プロキシシステムは、前記特定ユーザに付随するコンピュータシステムとは異なるネットワークアドレスを有するコンピュータシステムであることを特徴とする請求項28の周辺プロキシシステム。

【請求項30】 前記中央プロキシシステムは、前記特定ユーザ宛の電子メールを格納することが可能なデータ記憶領域をさらに有することを特徴とする請求項20の周辺プロキシシステム。

【請求項31】 前記第1ルーチンは、前記特定ユーザから受信されるデータに擬似ランダム関数およびハッシュ関数を適用することによって前記特定代用識別子を生

成することを特徴とする請求項20の周辺プロキシシステム。

【請求項32】 前記中央プロキシシステムは、前記特定ユーザに対する、前記サーバサイトに固有の電子メールボックスを格納することが可能なデータ記憶領域をさらに有することを特徴とする請求項20の周辺プロキシシステム。

【請求項33】 前記電子メールボックスは付随する鍵を有し、該鍵は前記データとインデックス番号の関数であることを特徴とする請求項32の周辺プロキシシステム。

【請求項34】 前記中央プロキシシステムは、与えられた特定代用識別子に対して、複数の電子メールボックスに格納された前記特定ユーザ宛の電子メールを収集するコンピュータ実行可能なルーチンをさらに有することを特徴とする請求項20の周辺プロキシシステム。

【請求項35】 前記中央プロキシシステムは、前記閲覧コマンドにセッションタグを付加するコンピュータ実行可能なマーカーチンをさらに有し、該セッションタグを使用して、前記特定代用識別子を各閲覧コマンドと関連づけることを特徴とする請求項20の周辺プロキシシステム。

【請求項36】 前記中央プロキシシステムは、前記サーバサイトがアクセス可能な、前記特定ユーザに固有のセッション情報を格納することが可能なデータ記憶領域をさらに有することを特徴とする請求項20の周辺プロキシシステム。

【請求項37】 前記中央プロキシシステムは、電子支払い情報を格納することが可能なデータ記憶領域をさらに有し、前記特定ユーザは、該電子支払い情報を使用して前記サーバサイトとの匿名商取引を行うことを特徴とする請求項20の周辺プロキシシステム。

【請求項38】 ユーザによって閲覧されることが可能なサーバサイトを有するネットワークとともに使用され、前記ユーザがプロキシシステムを通じて匿名的に前記ネットワーク上のサーバサイトを閲覧することを可能にする方法において、

特定ユーザから受信されるデータから特定代用識別子を生成する生成ステップと、

前記特定代用識別子を前記サーバサイトへ送信する送信ステップと、

前記特定ユーザから受信される閲覧コマンドを前記サーバサイトへ再送する再送ステップとからなることを特徴とする、匿名的にサーバサイトを閲覧する方法。

【請求項39】 前記データは、前記特定ユーザによって供給される識別データおよびユーザ定義可能文字列からなることを特徴とする請求項38の方法。

【請求項40】 前記特定代用識別子は、特定代用ユーザ名および特定代用ユーザパスワードからなることを特徴とする請求項38の方法。

【請求項41】 前記データから前記特定ユーザに対する特定代用電子メールアドレスを生成するステップをさらに有することを特徴とする請求項38の方法。

【請求項42】 前記サーバサイトのアドレスから前記特定代用識別子を生成するステップをさらに有することにより、前記特定代用識別子は前記サーバサイトに固有なものとなることを特徴とする請求項38の方法。

【請求項43】 前記サーバサイトは、前記ユーザに少なくとも1つのウェブページを提示することが可能なワールドワイドウェブサイトであり、前記方法は、前記特定ユーザの指示の下で前記特定代用識別子を前記サーバサイトへ送信するステップをさらに有することを特徴とする請求項38の方法。

【請求項44】 前記送信ステップは、前記特定ユーザによってウェブページフィールドに供給される英数字コードに基づいて前記特定代用識別子を前記サーバサイトへ送信するステップを有することを特徴とする請求項38の方法。

【請求項45】 前記英数字コードはエスケープシーケンスとして構成されることを特徴とする請求項44の方法。

【請求項46】 前記閲覧コマンドのうち前記特定ユーザの識別を前記サーバサイトに明らかにする部分を除去するステップをさらに有することを特徴とする請求項38の方法。

【請求項47】 前記生成ステップは、前記特定ユーザに付随するコンピュータシステム上で実行され、前記送信ステップおよび前記再送ステップは、前記特定ユーザに付随するコンピュータシステムとは異なるネットワークアドレスを有するコンピュータシステム上で実行されることを特徴とする請求項46の方法。

【請求項48】 前記特定ユーザ宛の電子メールを格納するステップをさらに有することを特徴とする請求項38の方法。

【請求項49】 前記生成ステップは、前記特定ユーザから受信されるデータに擬似ランダム関数およびハッシュ関数を適用するステップを有することを特徴とする請求項38の方法。

【請求項50】 前記特定ユーザに対する、前記サーバサイトに固有の電子メールボックスを作成するステップをさらに有することを特徴とする請求項38の方法。

【請求項51】 前記電子メールボックスは付随する鍵を有し、該鍵は前記データとインデックス番号の関数であることを特徴とする請求項50の方法。

【請求項52】 与えられた特定代用識別子に対して、複数の電子メールボックスに格納された前記特定ユーザ宛の電子メールを収集するステップをさらに有することを特徴とする請求項38の方法。

【請求項53】 前記方法は、前記閲覧コマンドにセッションタグを付加するステップをさらに有し、前記プロ

キシシステムは、該セッションタグを使用して、前記特定代用識別子を各閲覧コマンドと関連づけることを特徴とする請求項38の方法。

【請求項54】 前記サーバサイトがアクセス可能な、前記特定ユーザに固有のセッション情報を格納するステップをさらに有することを特徴とする請求項38の方法。

【請求項55】 前記方法は、電子支払い情報を格納するステップをさらに有し、前記特定ユーザは、該電子支払い情報を使用して前記サーバサイトとの匿名商取引を行うことを特徴とする請求項38の方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークに関し、特に、ネットワーク上の個人化（パーソナル化）されたサーバリソースを匿名的にユーザが閲覧することを可能にするシステムおよび方法に関する。

【0002】

【従来の技術】周知のように、インターネットは、共通のプロトコルを用いて協働（協力）するネットワーク（例えば、公衆および私設のデータ通信ネットワークおよびマルチメディアネットワーク）の集合体が世界的なネットワークのネットワークを形成したものである。

【0003】近年、より効率的で、信頼性が高く、費用効果の高いコンピュータおよびネットワーキングツールが利用可能になることにより、多くの会社および個人（まとめて「ユーザ」という。）が、成長しつつある電子市場に関わることが可能になっている。コンピュータ産業全体が経験したテクノロジーにおけるはかりしれない利得により、これらのユーザは、パーソナルコンピュータ（PC）のような市販のコンピュータによって、情報処理および通信の需要を満たすことが可能となっている。この目的のために、PCメーカは、ほとんどのPCに、インターネットのようなネットワークを通じた通信に使用可能なインタフェースを装備させている。

【0004】インターネットは、顧客に情報およびサービスを提供するビジネスの主要な場所としての地位をますます増大させている。このようなビジネスのうちよく知られた例として、ニュースプロバイダ（例えば、www.cnn.com (Cable News Network)、www.nytimes.com (New York Times)、www.wsj.com (Wall Street Journal)、www.ft.com (Financial Times Magazine)、www.businessweek.com (BusinessWeek Magazine))、自動車メーカ（例えば、www.ford.com/us (フォード社)、www.gm.com (GM)、www.toyota.com (トヨタ)、書店（例えば、www.amazone.com (Amazon.com books))、ソフトウェアプロバイダ（例えば、www.microsoft.com (Microsoft社)）などの多くのものがある。

【0005】ほとんどの場合、このようなビジネスは、ワールドワイドウェブ上にホームページを開設する（す

なわち「ウェブサイト」。ワールドワイドウェブは、インターネットの論理的オーバーレイである。ウェブサイトは、販売促進、広告およびビジネス実行のために使用可能な、電子的にアドレス可能なロケーションである。電子的な顧客は、ウェブブラウザ（例えば、Netscape Navigator（登録商標）、Microsoft Internet Explorer（登録商標））を用いて、それらのウェブサイト上で提供される情報にアクセスする。

【0006】ますます多くのウェブサイトが、ユーザの好みに従って調整されたハイパーリンク（あるハイパーテキスト文書内のポイントから別の文書内のポイントあるいは同じ文書内の別の場所への参照あるいはリンクであって、しばしば目立つように（例えば、異なる色、フォントまたは書体で）表示される）および表示されるメッセージを有する、ユーザの関心にカスタマイズされた「個人化ウェブページ」を含むことが可能な個人化サービスを提供している。このような好みは、ユーザに、そのウェブサイトのアカウントを設定させることによって確かめることができる。これにより、ウェブサイトは、そのユーザがたどったハイパーリンクを追跡することによって、あるいは、ユーザとの明示的なダイアログを通じて、ユーザの以前の訪問に関する情報を記憶することができる。例えば、Wall Street Journalは、セクションの順序および選択をカスタマイズした「個人化ジャーナル」を各ユーザに提供している。アカウントを開設するためには、ユーザは一般に、ユーザ名、パスワード、電子メール（Eメール）アドレスなどを含むフォームを電子的に完成させなければならない。電子メールアドレスは、ウェブサイトが、ウェブサイト上でユーザに提供されない情報を送るために使用されることが多い。

【0007】一般にインターネットを通じて、そして特にワールドワイドウェブを通じての電子通信の秘密性が本質的に欠如しているため、秘密電子通信を保証することが可能なシステムが非常に有効であると長い間考えられている。この問題の例として、安全で秘密の（匿名の）状態でワールドワイドウェブを閲覧し、個人化サービスを提供するサイトを訪れたいと考える顧客について考える。この顧客は、複数のサイトに対して、真正の識別を明かさず、同じユーザ名、パスワードを再使用せずに、ウェブサイトにアカウントを開設したいと考える。顧客は、あるサイトでのセキュリティの破れが他のサイトに影響を与えるのを避けるために、複数のサイトで同じユーザ名およびパスワードを再使用しないようにする。さらに、これらのユーザ名およびパスワードを使用しないようにすることは、複数のサイトが共謀して顧客の情報を組み合わせて特定の顧客に関する一件書類を構成する可能性を制限する。

【0008】一般に、顧客は多くのウェブサイトを訪れるため、各ウェブサイトごとに新たなユーザ名およびパスワードを発明し記憶することは面倒となる。さらに、

多くのウェブサイトは、顧客に対して、ユーザ名およびパスワードとともに電子メールアドレスを要求するが、電子メールアドレスを入力することによって、顧客の識別が知られてしまう。

【0009】さらに、ウェブサイトがクライアントおよびビジターを追跡することを可能にする製品が市販されている。このような追跡は、ユーザによって自発的に情報が提供されたり、フォームが完成されたりしなくても、可能である。このようなシステムの例として、Open Market, Inc.から市販されているWebreporterや、Group Cortexから市販されているSiteTrackがある。その広告には次のように記載されている。

【0010】「誰があなたのサイトを訪れているかを識別します。実際に訪れた人数を記録します。彼らがたどったリンクを見つけ、その完全なパスを追跡します。ユーザがどのサイトからやってきてどのサイトへ行ったかが分かります・・・。」

【0011】これらの製品が可能となっているのは、ワールドワイドウェブが主に依拠しているハイパーテキストトランスポートプロトコル（HTTPプロトコル）により、特定の情報がユーザからウェブサイトへ返されるためである。この情報には、例えば、ユーザの電子メールアドレス、ユーザがやってくる前のウェブサイト、ユーザのソフトウェアおよびホストコンピュータに関する情報が含まれることが可能である。他の関連するユーザ情報は、一般にcookieと呼ばれるもの（ウェブサイトがユーザのブラウザに記憶させることが可能な情報）を用いてユーザのブラウザへ送ることも可能である。そのウェブサイト次に訪れると、ユーザのブラウザは、ユーザが知らないうちにウェブサイトに情報を返す。

【0012】

【発明が解決しようとする課題】以上のことから、衝突すると思われる2つの目的、すなわち、ユーザの秘密性およびユーザの識別を提供することを満たす、匿名の個人化されたウェブ閲覧を行う方式が、従来技術において必要とされていることが明らかである。

【0013】

【課題を解決するための手段】従来技術の上記の欠点を解決するため、本発明は、次の2つの機能を実行するプロキシシステムを実現する。

（1）ネットワーク内のサーバサイト（例えば、ウェブサイト、ジャンクションポイント、インテリジェントポータルデバイス、ルータ、ネットワークサーバなど）が、そのサイトを閲覧（アクセス、検索、読み出し、接続など）しているユーザの真正な識別を決定することができないようにする、ユーザ固有の識別子の自動置換。

（2）サーバサイトが、そのサーバサイトを閲覧しているユーザの真正な識別を決定することを可能にする閲覧コマンドに付随する他の情報の自動除去。

【0014】本発明の重要な特徴は、以上の機能が、サ

サーバサイトへの後続の訪問中にプロキシシステムによって一貫して実行されることである（同じ代用識別子がそのサーバサイトへの繰り返しの訪問で使用される。また、サーバサイトは、ユーザによって供給される情報とプロキシシステムによって供給される情報を区別することができないため、プロキシシステムはサーバサイトにとって透過的（トランスペアレント）である）。従って、本発明は、匿名閲覧のみならず、代用識別子の一貫した使用に基づいた個人化を実現する。

【0015】注意すべき点であるが、本願において「真正な」という用語は、正確な、実際の、認証された、少なくとも部分的に正しい、本物の、真の、などを意味し、「または」という用語は、および/またはの両方を含めて意味し、「～に付随する」という句およびその派生語は、～内に有する、～と相互接続される、～を含む、～内に包含される、～に接続する、～と結合する、～と通信する、～と並置される、～と協力する、～とインタリーブされる、～の性質である、～と関連する、～を有する、～の性質を有する、などを意味する。

【0016】以下でさらに詳細に説明するように、本発明の原理によれば、上記のようなユーザの秘密性およびユーザの識別という衝突する問題が、プロキシシステム、周辺プロキシシステム、および、ユーザがプロキシシステムを通じて匿名的にサーバサイトを閲覧することを可能にする代用識別子をサーバサイトに提供する方法によって、解決される。

【0017】一実施例では、本発明は、サーバサイトで受信されユーザにとって個人的な識別子に基づいてユーザによって閲覧されることが可能なサーバサイトを有するネットワークとともに使用するために、ユーザが中央プロキシシステムを通じて匿名的にサーバサイトを閲覧することを可能にする代用識別子をサーバサイトに提供する中央プロキシシステムが実現される。本発明のさまざまな実施例によれば、代用識別子は、ユーザサイトによって、または、中央サイトに付随するルーチンによって、適当に生成されることが可能である（代用識別子を生成する有効な方法（機能）については後述する）。例示的な中央プロキシシステムは以下のものを有する。

（１）ユーザに固有のデータから生成されるサイト固有の代用識別子を処理（受信、受容、取得、構成、生成、など）するコンピュータ実行可能な第１ルーチン。

（２）代用識別子をサーバサイトへ送信し、その後、ユーザから受信される閲覧コマンドをサーバサイトへ再送するコンピュータ実行可能な第２ルーチン。

（３）閲覧コマンドのうちユーザの識別をサーバサイトに明らかにする部分を除去（およびおそくは置換）するコンピュータ実行可能な第３ルーチン。

【0018】一実施例では、上記の２つの基本機能のうちの第１の機能は、中央プロキシシステムの外部で実行され、第２の機能については、少なくとも一部は、中央

プロキシシステム内で実行される。中央プロキシシステムは、代用識別子を適当に処理し転送し、ユーザを識別することになる他の情報を取り外すことによって、上記の基本機能のうちの第２の機能を直接実行する。Netcom（登録商標）のようなインターネットアクセスプロバイダ（ISP）や、America Online（登録商標）あるいはCompuserve（登録商標）のようなネットワーキングサービスは、中央プロキシシステムを使用して、ユーザによる閲覧コマンドの匿名再送を行うことが可能である。

【0019】「同じ」ユーザが「同じ」サーバサイトに対してプロキシシステムを次に使用することにより、プロキシシステムは同じ（サイト固有の）代用識別子を（直接または間接に）生成し使用することを理解することが重要である。一般に、プロキシシステムは、ユーザとサーバの間でメッセージを通信する通路として機能する。実施例によって、プロキシシステムは、匿名性を保証するために、ユーザがサーバへ通信するメッセージの一部を除去または置換することが可能である。

【0020】本発明の代替実施例は、サーバサイトで受信されユーザにとって個人的な識別子に基づいてユーザによって閲覧されることが可能なサーバサイトを有するネットワークとともに使用するように設計された周辺プロキシシステムの形で実現される。この周辺プロキシシステムは以下のものを有する。

（１）特定ユーザから受信されるデータから特定代用識別子を生成するコンピュータ実行可能な第１ルーチン。

（２）特定代用識別子を中央プロキシシステムへ送信するコンピュータ実行可能な第２ルーチン。中央プロキシシステムは、特定代用識別子をサーバサイトへ再送し、その後、特定ユーザから受信される閲覧コマンドをサーバサイトへ再送する。この実施例によれば、第１ルーチンは、少なくとも一部は、ユーザサイトに付随することが可能であり、これにより、複数のコンピュータシステムにわたって本発明の基本機能を分散させる。

【0021】

【発明の実施の形態】図１は、本発明の原理を適切に使用することにより中央または周辺プロキシシステムが実現される、例示的な分散ネットワーク（全体的に１００で示す）の高水準ブロック図である。分散ネットワーク１００は、例えばインターネット１１５によって接続された複数のコンピュータサイト１０５～１１０を有する。インターネット１１５はワールドワイドウェブを含む。ワールドワイドウェブは、ネットワーク自体ではなく、ブラウザ、サーバサイト、HTMLページなどの組合せによってインターネット１１５上に維持される「抽象概念」である。

【0022】実施例によれば、各プロキシシステムは、ネットワーク１００の複数のサーバサイト１１０に代用識別子を提供する。代用識別子により、ユーザサイト（従ってユーザ（図示せず））は、プロキシシステムを

10

20

30

40

50

通じて匿名的にサーバサイトを閲覧することが可能となる。同じ（サイト固有の）代用識別子を特定サーバサイトで一貫して使用することにより、閲覧が個人化される。説明のため、サイト105aは本明細書を通じてユーザサイトであると仮定し、サイト110aは中央ブロキシサイトであると仮定し、サイト110gはサーバサイトであると仮定する。

【0023】当業者には理解されるように、図1は単なる例示であり、他の設定では、サイト105~110は、ユーザ、中央ブロキシもしくはサーバサイト、また

はこれらのうちの少なくとも2つの組合せであることが可能である。「サーバサイト」という用語は、ここでは広義に解釈するものとし、閲覧されることが可能な任意のサイトを含む。

【0024】実施例はインターネット115上で実装され使用されるのに適しているが、本発明の原理および技術的範囲は、有線か無線にかかわらず、サーバサイトで受信されユーザにとって個人的な識別子に基づいてユーザによって閲覧されることが可能なサーバサイトを有する適当に構成されたコンピュータ、通信、マルチメディアなどのネットワークで実現可能である。さらに、本発明の原理について、単一のユーザサイト105a、単一の中央ブロキシサイト110aおよび単一のサーバサイト110gを用いて説明するが、別の実施例では複数のユーザ、中央ブロキシまたはサーバのサイトを含むことも可能である。

【0025】ネットワーク100は、ネットワーク100のサイト105~110どうしを相互接続するように動作する安全でない複数の通信チャネルを有すると仮定される。通信チャネルの概念は既知であり、相互接続されるサイト間で情報の安全で内通信を行う（インターネットは、周知の通信プロトコルを使用する）。分散ネットワークオペレーティングシステムが、少なくともいくつかのサイト105、110上で実行され、サイト間での情報の安全で内通信を管理する。分散ネットワークオペレーティングシステムも既知である。

【0026】本発明の中央ブロキシシステム110a（詳細は図2に関して後述する）によれば、代用識別子は、中央ブロキシシステム110aによって、適切に間接的にサーバサイト110gに提供される（代用識別子によって、ユーザサイト105aは、サーバサイト110gを匿名的に閲覧することが可能となることを想起すべきである）。サイト固有の代用識別子は、ユーザ105aに固有のデータから、ユーザ105aまたは中央ブロキシシステム110aのいずれかによって適切に提供あるいは生成される。中央ブロキシシステム110aは、複数の実行可能ルーチンを有する。第1ルーチンは、ユーザ105aに固有のデータからサイト固有の代用識別子を生成する（サイト固有の代用識別子は、中央ブロキシサイト110aによって（例えば、中央ブロキシ

シシステム110aに付随するルーチンによって）、適切に生成されることが可能である）。第2ルーチンは、代用識別子をサーバサイト110gへ送信し（おそらくは複数の中間のユーザサイトおよびサーバサイト105、110を介して）、その後、ユーザサイト105aから受信される閲覧コマンドをサーバサイト110gへ再送する。第3ルーチンは、閲覧コマンドのうちユーザの識別をサーバサイト110g（および複数の中間のユーザサイトおよびサーバサイト105、110）に明らかにする部分を除去（およびおそらくは置換）する。ここで、「ルーチン」という用語は広義に解釈されるものであり、プログラム、手続き（プロシージャ）、オブジェクト、タスク、サブルーチン、関数、アルゴリズム、命令セットなどのような通常の意味を含むのみならず、命令の列や、機能的に等価なファームウェアおよびハードウェア実装をも含むものである。

【0027】あるいは、本発明の周辺ブロキシシステム（全体的に120で示す）（これについて詳細は図5に関して後述する）は、サーバサイト110gで受信されユーザサイト105aにとって個人的な代用識別子に基づいてユーザサイト105aによって閲覧されることが可能なサーバサイト110gを有するネットワーク100で使用するよう設計される。周辺ブロキシシステム120は、第1および第2の実行可能ルーチンを有する。第1ルーチンは、ユーザサイト105aまたは中央ブロキシシステム110aに存在し、ユーザサイト105aに固有のデータから特定代用識別子を生成する。第2ルーチンは、ユーザサイト105a、または、部分的にユーザサイト105aおよび中央ブロキシシステム110aに存在し、特定代用識別子を中央ブロキシシステム110aに送信する。その後、中央ブロキシシステム110aは、特定代用識別子をサーバサイト110gへ再送し、その後、ユーザサイト105aとサーバサイト110gの間で情報（例えば、閲覧コマンド、データなど）を通信（例えば、送信、受信など）する。

【0028】実施例によれば、周辺ブロキシシステム120は、第1および第2のルーチンの実行のロケーションにおいて、中央ブロキシシステム110aと異なる。中央ブロキシ実施例では、すべてのルーチンは中央ブロキシシステム110aで実行される。これは、すべてのユーザがユーザ固有の情報を中央ブロキシシステム110aに送らなければならないことを意味する。周辺ブロキシシステム120の実施例では、第1および第2のルーチンはユーザサイト105aに付随するブロキシサブシステムで実行されることが可能である。一実施例では、ユーザシステム105aのユーザ固有情報（例えば、ユーザの識別、パスワード、電子メールアドレス、電話番号、クレジットカード番号、郵便アドレスなど）はローカルのままであり、一般に、中央ブロキシシステム110aよりも安全となる。

【0029】上記のように、Netcom（登録商標）のようなISPや、America Online（登録商標）あるいはCompuserve（登録商標）のようなネットワーキングサービスは、いずれかのプロキシシステム（中央または周辺）を使用して、ユーザサイトとサーバサイトの間での閲覧（例えば、アクセス、選択、読み出しなど）コマンドの匿名通信（送信、受信、再送など）を提供することが可能となる。

【0030】上記の実施例の重要な特徴は、サイト固有の代用識別子を使用することにより、ユーザが、アカウントの開設を要求する各サーバサイト（例えば、New York Times、Wall Street Journal、Newspage（登録商標）およびESPN（登録商標）のサイト）ごとに新たなユーザ名およびパスワードを「発明」する必要がなくなることである。実施例は、別個の、ユーザにとって安全な代用識別子（例えば、エイリアスのユーザ名、パスワード、電子メールアドレス、郵便アドレス、クレジットカード番号など）を生成する。ユーザは、例えばプロキシシステムセッションの開始時に、1個以上の文字列（ランダムでもよい）を与える。プロキシシステムは、それを用いて、そのユーザに対する安全なサイト固有の代用識別子を生成する。これにより、ユーザは、各サーバサイトごとに新たな固有の識別子を発明する負担から解放される。さらに、ユーザは、特定のサーバサイトがアカウントを要求するのに応答するたびにこのような安全な識別子をタイプ入力する必要がなくなる。その代わりに、プロキシシステムが、自動的に適当な安全な識別子を提供する。実施例では、プロキシシステムは、サーバサイトの閲覧中に、ユーザサイト105aから送られる他の識別情報（例えば、HTTPヘッダなど）をフィルタリングする。サーバサイトは一般に、プロキシシステム110aによって供給される情報と、ユーザサイト105aによって供給される情報を区別することができないことに留意することが重要である。すなわち、中央プロキシシステム110aは、サーバサイトにとって透過的である。

【0031】一実施例では、代用識別子は、サーバからの要求に応じて、ユーザからの介在なしに送信される。このプロセスは、ワールドワイドウェブ上でユーザを識別するためにサーバによって使用される一般的な手続きである「基本認証要求」への応答を自動化する。このようにして、ユーザはこの活動による負担を受けない。

【0032】実施例によれば、代用識別子を生成するため、プロキシシステムは、ユーザ定義可能文字列の形で秘密情報（少なくとも1つのサーバサイトにとって秘密な）を適当に管理する。この文字列は、ユーザによって定義され、プロキシシステムに付随するメモリに記憶するというような通常の方法で管理される。あるいは、ある関数（後述）を用いて、少なくとも一部は秘密情報に付随する代用識別子を生成することも可能である。1つ

のアプローチによれば、プロキシシステムは、データベース、データレポジトリ、配列など、あるいは、ユーザ情報を置換（エイリアス）識別子にマッピングするために用いられるエイリアステーブルのような、通常の日付構造を管理することにより、代用識別子を管理する。

【0033】一実施例によれば、ユーザは、各セッションの開始時に、自己の秘密（ユーザ定義可能文字列）を発信する。これは、プロキシシステムによって、直接または間接に、そのセッションの代用識別子を生成するために使用される。このオプションは、ユーザが異なるときに異なるプロキシを選択する自由度を有し、プロキシシステムに記憶される恒久的な秘密情報がないという点で有利である。別の関連実施例では、データは少なくとも2つの秘密のユーザ定義可能文字列からなり、第1ルーチンはその少なくとも2つの秘密のユーザ定義可能文字列から一部が生成される代用識別子処理する。もちろん、本発明に従って、別の適当なアプローチを用いて、匿名の個人化ウェブ閲覧を実現する目的を達成することも可能である。

【0034】図2は、分散ネットワーク100のサブネットワーク（全体的に200で示す）のブロック図である。本発明の原理に従って、サブネットワーク200は、ユーザサイト105a、中央プロキシシステム110aおよびサーバサイト110g（インターネット115の他の複数のサーバサイト110とともに示す）を有する。

【0035】説明のため、ユーザサイト105aは、サーバサイト110g（New York Tribuneウェブサイト（NYT））にアクセスするコマンドを発行すると仮定する。このようなアクセスは、中央プロキシシステム（サーバサイト）110aを介して行われ、これにより、ユーザサイト105aに関するユーザ固有データがインターネット115の残りの部分に通信されないことが保証される。例えば、ユーザサイト105aに関するデータを含むHTTPヘッダフィールドがあれば、中央プロキシシステム110aがフィルタリングする。

【0036】中央プロキシシステム110aは、インターネット115の他のサイトを介さずユーザサイト105aに接続するサーバサイト上で実行される。実施例によれば、中央プロキシシステム110aは、ユーザサイト105aから、物理的にも論理的にも、適当に離れていることが可能である。サーバサイトは、要求をしたマシンのIP (Internet Protocol) アドレスを物理的および論理的に決定することができるため、ユーザサイト105aはサーバサイトに直接アクセスすることはない。

【0037】実施例によれば、NYT110gにアクセスするユーザサイト105aのコマンドがユーザサイト105aの現在のセッションの最初の要求である場合、中央プロキシシステム110aは、それを認識し、おそ



らしくはユーザサイト105aのブラウザに自己のHTML文書を表示する。

【0038】図3を参照すると、本発明の原理に従って、中央プロキシシステム110aのはめ込まれたインタフェース305 (Janus<sup>SM</sup>) を表示する通常のブラウザ300 (Netscape (登録商標)) のフルスクリーンウィンドウが示されている。インタフェース305は、サイト105aのユーザに、ユーザ定義可能文字列を入力するよう要求する。ユーザ定義可能文字列は、実施例によれば、ユーザによって供給される識別(ID)データおよび秘密(S)データである。各ユーザは、まず、ユーザID (例えば、電子メールアドレス) およびユーザSを供給することにより、代用識別子が選択あるいは生成されることを可能にする(サイト固有の代用識別子は、ユーザ105aと、ユーザ105aが閲覧しようとしている特定サーバサイトとに固有のデータから適切に生成される)。あるいは、アプリケーションによっては、ユーザによって供給される他のデータ(例えば、クレジットカード番号、郵便アドレス、ハンドルなど)も適当である。

【0039】実施例によれば、代用識別子は、適当な関数を用いて構成(生成)される。この関数は、匿名性、一貫性、衝突耐性および一意性、一件書類の作成からの保護、ならびに、単一の秘密および受容可能性の特徴を有する。匿名性に関して、ユーザの識別は秘密に保たなければならない。すなわち、サーバサイト、あるいは、サイトの連合が、代用識別子からユーザの真正な識別を決定することはできない。一意性に関して、各サーバサイトごとに、各ユーザに代用識別子が提供され、サーバサイトは、この代用識別子が与えられるとユーザを認識することが可能であることにより、ユーザのアクセスを個人化することが可能となり、こうしてユーザはサーバサイトに「登録」されることが可能となる。

【0040】衝突耐性および一意性に関して、与えられたユーザの識別およびサーバサイトに対して、第三者が、そのサーバサイトに対する同一のエイリアス(なりすまし)につながるような別のユーザ識別を発見してはならない。一件書類の作成からの保護に関して、ユーザは、異なるサーバサイトに対して異なるエイリアス(代用識別子)を割り当てられることにより、サイトの連合が、ユーザによってアクセスされたサイトのセットに基づいてユーザの習慣を知りユーザプロファイル(一件書類)を作成することはできない。最後に、単一の秘密(ユーザ定義可能文字列)および受容可能性により、与えられたユーザの識別および単一の秘密に対して、安全で別個のエイリアス(代用識別子)が、各サーバサイトごとに、ユーザにとって透過的に、必要に応じて自動生成される。ユーザの観点からは、ユーザ定義可能文字列は、サーバサイトの集合体に対する普遍的なパスワードと透過である。

【0041】本実施例によれば、反対者(ユーザを識別しようとするサーバサイト)Eがユーザの秘密Sを読むことができた場合、ユーザIDは「破られている」(秘密でない)。あるいは、Eがエイリアスパスワードを読むことができた場合、特定サーバサイトwに関してユーザIDは「部分的に開かれている」(完全に安全ではない)。ユーザIDが部分的に開かれ、かつ、Eがエイリアスパスワードをエイリアスユーザ名とともにユーザIDに関連づけることができた場合、wに関してユーザIDは「開かれている」(安全でない)。関数T()が以下のように定義されると仮定する。T(ユーザ名、ウェブサイト(w)、S)=(代用ユーザ名、パスワード)。すなわち、 $T(id, w, S) = (Uw, Pw)$ と定義する。また、 $Tu(id, w, S) = Uw$ および $Tp(id, w, S) = Pw$ と定義する。

【0042】 $Tu(id, w, S) = Uw = h(enc(k, id, f(s_1, w)))$

$Tp(id, w, S) = Pw = h(enc(k, id, f(s_2, w)))$

である。ただし、

id: ユーザサイト105aのID (例えば電子メールアドレス) を表す。

w: サーバサイト110gのドメイン名を表す。

//: 接続の論理演算を表す。

S:  $k // s_1 // s_2$ 、すなわち、ユーザサイト105aの定義可能文字列を表す。

xor: 排他的論理和のブール演算を表す。

f(k, x): 擬似乱数値を生成するように適当に構成された関数を表し、des(k, h(x), x)のような関数の群から選択することが可能である。

enc(k, x, r):  $r // (f(k, r) \text{ xor } x)$ を表す。

h(): MD5のような、衝突耐性のあるハッシュ関数を表す。

des(k, i, x): 情報xの暗号ブロック連鎖(CBC)モードにおける、鍵kおよび初期化ベクトルiを用いたDES暗号化(既知)を表す。

Tu()およびTp()はいずれも、ハッシュ関数

h()の結果を適当に切り詰めて、特定サーバサイトに対して許容される最長のユーザ名あるいはパスワードに合わせることが可能である。

【0043】この関数T()を上記の特徴に関係づける以下ようになる。

1. Eは、部分的に開かれているのみであって破られていないユーザの識別IDを推量することができるだけである。

2. T()は決定性関数であり、Eは、開かれておらず破られていないユーザのエイリアスパスワードを推量することができるだけである。

3. 与えられたwと、破られておらず開かれていないユ

ーザIDとに対して、EはIDおよびSを推量することができるだけである。

4. 破られていないユーザIDおよびwに対して、 $T(id, w, S)$ は、wに等しくないw' に対する $T(id, w', S)$ に関する情報をEに与えない。

5.  $T(id, w, S)$ の値域は、正しいユーザ名およびパスワードとしてサーバサイトによって受容されるようなものである。これは、制限された長さの印字可能文字列を意味する。

当業者には理解されるように、本発明の原理に従って、上記の通りの他の適当な関数を代用することも可能である。

【0044】上記の代用識別子生成関数、および、これに関する限り、本発明に従って代用識別子を生成する他の適当に構成された関数を使用することは、匿名化され個人化された閲覧という上記の特徴を実現するように作用する。本発明によれば、はじめにサイト固有の代用識別子によってサーバサイトを匿名的に訪れ、その代用識別子の関数としてサーバサイトと対話し、後の機会に同一のサイト固有の代用識別子を用いてそのサーバサイトを再訪問し、認識された代用識別子の関数として（おそらくは個人化された処置を受けて）再来の顧客としてそのサーバサイトと対話する。略言すれば、代用識別子は一貫して生成され、実施例ではサイト固有のものとして生成される。

【0045】本発明の一実施例では、代用識別子は、サイト固有の代用ユーザ名およびサイト固有の代用ユーザパスワードを含む。「サイト固有」とは、おそらくは各サイトのアドレスに依存して、名前およびパスワードがサイトごとに異なることを意味する。これは、与えられたユーザに関する一件書類を作成する作業を複雑にする。関連実施例では、第1ルーチンは、サイト固有データからユーザサイト105aに対するサイト固有の代用電子メールアドレスを生成する。代替実施例では、第1ルーチンは、サーバサイトのアドレスからサイト固有の代用識別子を生成する。もちろん、サイトのアドレス以外のサイト固有の情報を用いて代用識別子を生成することも可能である。

【0046】ユーザが中央プロキシシステム110aに最初に接続された場合、ユーザは、ランダムに適当にユーザ定義文字列（秘密）を生成し、それをローカルに記憶する。一実施例では、第1ルーチンは、ユーザサイト105aから受信されるデータに擬似ランダム関数およびハッシュ関数（例えば、上記の $T()$ 関数）を適用することによって生成される代用識別子进行处理する。当業者には、擬似ランダム関数およびハッシュ関数の構成および操作ならびにその使用法は周知である。本実施例および関連実施例の重要な特徴は、本発明が、現在の関数および将来発見される関数を利用して匿名性およびセキュリティを改善することができることである。

【0047】あるいは、現在のセッションの最初の接続である場合、ユーザは、記憶されているユーザ定義文字列を中央プロキシシステム110aに適当に送ることも可能である。それにもかかわらず、ブラウザ300は、インタフェース305を、ユーザのIDおよびその他のユーザ定義可能文字列とともに中央プロキシシステム110aに送信する。中央プロキシシステム110aは、この情報を受信し、それをセッションの残りの部分で使うことが可能である。

【0048】一実施例では、第1ルーチンは、閲覧コマンドに付加されるセッションタグを受信または生成し、中央プロキシサイト110aは、セッションタグを使用して、代用識別子を各閲覧コマンドと関連づける。セッションタグは、本発明に必須ではないが、ユーザサイト105aがデータを一度だけ（通常は各セッションの開始時に）供給することを可能にする1つの手段を提供する。関連実施例では、中央プロキシサイト110aは、ユーザサイト105aに固有のセッション情報を含むことが可能でありサーバサイト110gがアクセス可能なデータ記憶領域を有する。

【0049】一実施例では、上記の第2ルーチン（中央プロキシシステム110aにローカルなものとすることが可能である）は、代用識別子をサーバサイト110gへ送信する。別の実施例では、第2ルーチンは、ユーザによってウェブページ305のフィールドに供給される英数字コードに基づいてサーバサイト110gへ代用識別子を送信する。この英数字コードは、第2ルーチンに対して、代用識別子をどのようにしてどこに見つけるかを知らせ、ユーザが、代用識別子を直接提供しなければならないことのないようにする。関連実施例では、ユーザはウェブページ305のフィールドに英数字コードを手入力する。もちろん、本発明は、ウェブページ305のフィールドの知的解析により英数字コードをどのようにしてどこに見つけるかを自動的に決定することも含む。当業者には、一般にインターネットは周知であり、特に、ワールドワイドウェブと、ワールドワイドウェブの構造が「閲覧（ブラウジング）」を促進する方法については周知である。本発明は、インターネットおよびワールドワイドウェブにおいて有用であると考えられるが、当業者には直ちに理解されるように、本発明は、適当に設定されたコンピュータ、通信、マルチメディアなどのネットワーク構成においてインターネット以外のアプリケーションでも有効である。

【0050】中央プロキシシステム110aがユーザに関する必要な情報を取得した後、上記の第3ルーチンは、閲覧コマンドのうちユーザサイト105aの識別をサーバサイト110gに明らかにする部分を除去し、ユーザサイト105aのものとアクセス要求をNYTサイト110gへ（例えば、HTTPのgetリクエストを用いて）転送する。これにより、要求（リクエスト）か

ら、ユーザの識別を明らかにする可能性のあるヘッダフィールドなどが選択的に除去される。

【0051】これがNYTサイト110gへのユーザの最初の訪問である場合、NYTサイト110gはユーザに電子フォームを提供し、アカウントを開設するために、例えば、ユーザ名、パスワード、および電子メールアドレスの人力を要求する。図4を参照すると、本発明の原理に従って、サーバサイト110gのはめ込まれたインタフェース400 ("The New York Tribune") を表示する通常のNetscape (登録商標) ブラウザ300のフルスクリーンウィンドウが示されている。

【0052】ここで、固有のユーザ名および秘密のパスワードを入力しなければならない代わりに、ユーザは、簡単なエスケープ文字列 (例えば、<uuuu>および<pppp>) をこれらのフィールドに入力する。具体的には、上記の英数字コードをこのようなエスケープシーケンスに適切に設定することが可能である。当業者にはエスケープシーケンスは周知である。これらの文字列は、中央プロキシサイト110aによって認識される。中央プロキシサイト110aは、ユーザサイト105aのユーザ名および秘密 (ユーザ定義可能文字列) ならびにNew York Tribuneのドメイン名を使用して、例えば関数T (ID, 秘密, ドメイン名) によって、代用識別子 (例えば、図2のエイリアスユーザ名u3およびエイリアスパスワードp3など) を計算する。サイト固有の代用識別子は、ユーザが特定サーバサイトに入力するのと同じ機構を用いて、中央プロキシシステム110aによって特定サーバサイトに送られる。換言すれば、プロキシシステム110aは、ユーザサイト105aからサーバサイト110g宛の情報通信 (例えば、閲覧コマンド) を受信し、それをサーバサイト110gへ再送する。すなわち、中央プロキシシステム110aは、匿名化のための透過的な通路として作用するとともに、サイト固有の代用識別子の一貫性のある生成を通じて、サーバサイト閲覧の個人化を行う。

【0053】後でNYTサイト110gを訪れると、ユーザサイト105aは (中央プロキシシステム110aによってNYTサイト110gへ転送された最初のgetリクエストに応答して) 自己を認証することを要求されるが、中央プロキシシステム110aは、自動的にu3およびp3を再計算し、NYTサイト110gにこれらの値を返送 (getリクエストの再送) することによって応答するように適切に動作する。これにより、ユーザサイト105aは、NYT110gアカウントのユーザ名およびパスワードを記憶する負担から解放される。要するに、ユーザサイト105aを巻き込まずに適切に実行されるプロトコルは、以下の通りである。

(1) NYTサイトサーバ110gが、最初のgetリクエストに失敗することによって中央プロキシサイト110aからの認証を要求する。

(2) 中央プロキシサイト110aは代用識別子 (例えば、エイリアスユーザ名、エイリアスパスワード) = T (ID, 秘密, ドメイン名)、などを再計算する。

(3) 中央プロキシサイト110aは、この代用識別子とともにgetを再送信することによって応答する。

【0054】代用識別子は、ユーザ105aによる同じサーバサイトへの後の訪問でも提示されるという意味で一貫性がある。一貫性のある代用識別子により、サーバサイトは、再来したユーザを認識し、そのユーザに個人化されたサービスを提供することが可能となる。一実施例では、第2ルーチンは、サーバからの要求に応じて、ユーザ105aからの介在なしに、代用識別子を送信する。このプロセスは、ワールドワイドウェブ上でユーザを識別するためにサーバによって使用される一般的な手続きである「基本認証要求」への応答を自動化する。このようにして、ユーザ105aはこの活動による負担を受けない。本実施例では、第2ルーチンは、代用識別子とともにもとのユーザ要求をサーバへ再送する必要がある可能性もある。

【0055】注意すべき点であるが、多くのサーバは、アカウントを作成するために正しい電子メールアドレスを要求する。真正な電子メールアドレスはユーザを一意的に識別してしまうため、ユーザはそれをこの目的に使用することはできない。本発明のプロキシシステムは、ユーザサイト105aのエイリアス電子メールアドレスを作成することによってこの問題を適切に解決し、電子メールを電子メールボックスに記憶する。一実施例では、中央プロキシシステム110aは、ユーザ宛の電子メールを格納することが可能なデータ記憶領域を有し、それにより、サーバがユーザに直接接続することがなくなる。従来の匿名リメーラとは異なり、本実施例は、中央プロキシシステム110aにエイリアスから真正なユーザ識別子への変換テーブル (これは大きく無防備となることがある) を記憶する必要がない。本実施例では、中央プロキシシステム110aが変換テーブルを管理し保護する必要がなく、そのようなテーブルの内容を第三者に知られこともないため、本実施例は従来技術のアプローチよりも本質的に安全である。

【0056】代替実施例では、中央プロキシシステム105aはさらに、ユーザごとにサーバサイト固有の電子メールボックスを格納することが可能なデータ記憶領域を有する。本実施例によれば、各ユーザは、そのユーザ宛のメールを生成した各サイトごとにメールボックスを有する。ユーザへの自動メール再送によってセキュリティを危険にさらすのではなく、本実施例は、各ユーザが明示的に取得するように電子メールを記憶する。

【0057】ユーザは、各サーバごとに、おそらくはユーザ代用識別子によって識別される別々の電子メールボックスを設けると有効である。このアプローチにより、第三者から受信される電子メールメッセージ (例えば、

ジャンク電子メール)を適切に廃棄するとともに、電子メールメッセージの選択的廃棄も可能となる。

【0058】一実施例では、各電子メールボックスは付随する鍵を有する。この鍵は、データとインデックス番号の関数である。電子メールボックスでの鍵の使用は既知である。別の実施例では、中央ブロキシシステム110aはさらに、与えられた代用識別子に対して、ユーザ宛の、複数のサイト固有電子メールボックスに格納された電子メールを収集するコンピュータ実行可能ルーチンを有する。この実施例は、ユーザが適当なデータを供給すると、ユーザサイト105aのさまざまなメールボックスを自動的に検索し、そこからメールを取得するメイン収集ルーチンを適切に使用することが可能である。

【0059】一実施例によれば、中央ブロキシシステム110aは、電子支払いをサポートするのに必要な機能を有し、ユーザは、電子支払い情報を使用して、サーバサイトとの匿名商取引を行う。これを実現するため、中央ブロキシシステム110aは、このような電子支払い情報を格納することが可能なデータ記憶領域を有する。さらに、代用識別子は、少なくとも一部は、クレジット／デビットカード番号、銀行支店あるいは口座番号、郵便アドレス、電話番号、課税識別番号、社会保険番号などを用いて生成される。匿名商取引を実現するさまざまな方法は既知である。

【0060】別の例として、ますます多くのサイトが、ユーザにサービスの課金を行うことができるように、アカウントの開設の一部として正しいクレジット番号を要求する(例えば、Wall Street Journal(登録商標)、ESPN(登録商標)、など)。上記のブロキシシステムは、代用識別子により、ユーザがこれらの事項を記憶することからユーザを解放し、ウェブサイトへ(不本意に)データが流れることに対する保護を提供しているが、クレジットカード番号をサイトに提供したユーザに対する完全な匿名性を提供するものではない。1つの解決法は、既に簡単に説明したように、中央ブロキシシステム110aが、自己の正しいクレジットカード番号を要求側サイトに提供した後、ユーザから金額を収集することである。中央ブロキシシステム110aがインターネットプロバイダに組み込まれている場合(例えば、America Online(登録商標)のように)、この関係は既に存在する。

【0061】あるいは、中央ブロキシシステム110aは、他のサイトから知られ信頼されていることにより、中央ブロキシシステム110aは、エイリアスクレジットカード番号および満期日を生成して、このデータを認証し、要求側サイトに送ることも可能である。その後、サイトはこの番号が実際に中央ブロキシシステム110aから発信されたことを検査し、それを正しいものとして受容し、中央ブロキシシステム110aから金額を収集することができると理解する。もはや、中央ブロキシ

システム110aとサイトの間で「真の」クレジットカード番号を送る必要はない。

【0062】上記の実施例のさまざまな特徴は、図1に記載した周辺ブロキシシステムでも適切に実現されることを認識することが重要である。具体的には、図5を参照すると、図1の分散ネットワークのサブネットワーク(全体的に500で示す)のブロック図において、周辺ブロキシシステム120が示されている。本発明の原理によれば、サブネットワーク500は、各ユーザサイト105aと、中央ブロキシシステム110aと、NYTサイト110g(インターネット115の複数のサーバサイト110とともに示す)を有する。

【0063】上記のように、周辺ブロキシシステム120は、第1および第2の実行可能ルーチンを有する。第1ルーチンは、ユーザサイト105aに存在し、ユーザサイト105aに固有のデータから代用識別子を生成する。第2ルーチンは、実施例では同じくユーザサイト105aに存在し、代用識別子を中央ブロキシシステム110aへ送信する。中央ブロキシシステム110aは、代用識別子をサーバサイト110gへ再送し、その後、ユーザサイト105aとサーバサイト110gの間で情報(例えば、閲覧コマンド、データなど)を通信(例えば、送信、受信など)する。この第2の構成は、ユーザが中央ブロキシシステム110aあるいは間の通信ラインを信頼しておらず、ユーザの識別やその他の秘密情報を安全に保ちたい場合に特に有効である。

【0064】ローカルブロキシシステム510は、これを管理するために使用され、また、ユーザの識別およびその他の情報を用いて代用識別子を計算する。ローカルブロキシシステム510は、中央ブロキシシステム110aと通信する。中央ブロキシシステム110aは、サーバへの通信を転送し電子メールを処理するために使用される。一実施例では、中央ブロキシシステム110aは、ユーザに付随するコンピュータ実行可能なローカルルーチンと通信する。このローカルルーチンは、ユーザに固有のデータからサイト固有の代用識別子を生成する。中央ブロキシシステム110aは、各ユーザにとってローカルな分散ルーチンに基づくことが可能であり、その場合、分散ルーチンが、代用識別子を生成し、それを中央ブロキシシステム110aへ送信する。

【0065】次に、図6は、本発明のマーカブロキシ実施例による、各ユーザサイト105a、中央ブロキシシステム110aならびに複数のサーバサイト110b、110c、および110gを有する、分散ネットワーク100のサブネットワーク(全体的に600で示す)のブロック図である。上記のように、本発明の中央ブロキシシステムは、少なくとも2つの構成、すなわち、中央ブロキシ構成(図2)または周辺ブロキシ構成(図5)で使用可能である。

【0066】中央ブロキシ構成では、中央ブロキシシ

テム110aが代用識別子を計算する。この構成の実装では、ユーザサイト105aが、ユーザ定義可能文字列（例えば、ユーザの識別、パスワードおよびその他の秘密情報）を一度提供することが要求され、その後、中央プロキシシステム110aは、必要に応じて代用識別子を生成する。中央プロキシシステム110aは、ユーザ定義可能文字列を、同じユーザサイト105aによって生成される一連のHTTPリクエストと関連づける。中央プロキシシステム110aは、特定のユーザサイト105aと中央プロキシシステム110aの間のすべての通信を含む1つのセッションに各リクエストを関連づけることも可能である。

【0067】しかし、HTTPプロトコルは一般に、セッションおよびリクエスト間の関係を直接サポートしない。具体的には、各HTTPリクエストは新たなソケット接続で送られ、同じユーザからの引き続くリクエストをリンクすることができるHTTPヘッダフィールドは要求されない。

【0068】注意すべき点であるが、中央プロキシシステム110aは計算なしで通信を転送することが可能であるため、セッションの識別は一般に周辺プロキシ構成では不要である。代表的実施例では、周辺プロキシシステム120は、ユーザサイト105aから受信される閲覧コマンドを中央プロキシシステム110aへ再送し、中央プロキシシステム110aは、このコマンドをサーバサイト110gへ再送する。一実施例によれば、周辺プロキシシステム120は、閲覧コマンドのうちユーザサイト105aの識別をサーバサイト110gに明らかにする部分を除去（およびおそらくは置換）する。

【0069】一実施例では、ユーザサイト105aは、ローカルに、マークプログラム605を実行する。マークプログラム605は、ユーザサイト105aのリクエストにセッションタグを付けるように動作する。中央プロキシシステム110aは、このタグを用いて、ユーザ群の特定ユーザに属するリクエストを識別する。マークプログラム605は、ユーザサイト105aのセッションタグを記憶し、このタグにすべてのリクエストを付加するように実装されることも可能である。中央プロキシシステム110aは、サーバサイトへリクエストを転送する前にこのセッションタグを除去する。セッションタグは一意的であるべきであり、2人のユーザが同じタグを有してはならない。

【0070】注意すべき点であるが、Netscape（登録商標）は“cookie”を使用している。これは、長期的なセッション情報を記憶し取得するための機構である（“cookie”の使用は概念的には既知である）。cookieは、閲覧されるサーバによって生成され、特定のドメイン名に関連づけられる。ブラウザ300は、ユーザがそのドメインを再訪問するときに、特定のドメイン名に関連づけられたcookieを送信する。サーバは一般に、自己のドメイン

に付随するcookieを生成するのみである。cookieは、「ショッピングカート」、アカウント名、パスワード、イベントカウンタ、ユーザ初期設定などのようなセッション情報を保持する簡単な機構を提供する。

【0071】会社によっては、ユーザおよびその習慣を追跡するためにcookieを広範に使用している。本発明のプロキシシステムは、閲覧されるサーバに代用識別子を提示するため、サーバは、真のユーザ識別を知ることができない。こうして、サーバがcookieに格納するすべての情報は「別人」に関するものであり、真のユーザに関するものではない。ユーザが同じサーバに戻るときには、同じ代用識別子が提示され、この別人に対して以前にサーバが生成したcookieも提示される。

【0072】上記から明らかなように、本発明は、ユーザサイトおよびサーバサイトを有するネットワークとともに使用される。サーバサイトは、サーバサイトで受信されユーザサイトにとって個人的な識別子に基づいてユーザサイトによって閲覧されることが可能である。本発明によれば、ユーザサイトが中央プロキシシステムを通じて匿名的かつ個人的にサーバサイトを閲覧することを可能にする、一貫性のある代用識別子をサーバサイトに提供する中央プロキシシステムおよび周辺プロキシシステムが実現される。

【0073】例示的な中央プロキシシステムは以下のものを有する。

(1) ユーザサイトに固有のデータから生成されるサイト固有の代用識別子进行处理する実行可能な第1ルーチン。

(2) 代用識別子をサーバサイトへ送信し、その後、ユーザサイトから受信される閲覧コマンドをサーバサイトへ再送する実行可能な第2ルーチン。

(3) 閲覧コマンドのうちユーザサイトの識別をサーバサイトに明らかにする部分を除去（およびおそらくは置換）する実行可能な第3ルーチン。

【0074】例示的な周辺プロキシシステムは以下のものを有する。

(1) 特定ユーザサイトから受信されるデータから特定代用識別子を生成する実行可能な第1ルーチン。

(2) 特定代用識別子を中央プロキシシステムへ送信する実行可能な第2ルーチン。その後、中央プロキシシステムは、特定代用識別子をサーバサイトへ再送し、その後、特定ユーザサイトから受信される閲覧コマンドをサーバサイトへ再送する。

【0075】以上、本発明について詳細に説明したが、当業者であれば、本発明の原理に基づいてさまざまな変形例を実施することが可能である。具体的には、当業者には明らかなように、上記のルーチンはソフトウェアによるものであり、適当な通常のコンピュータシステムあるいはネットワークで実行可能である。本発明の別の実施例は、少なくとも一部は、ファームウェアもしくはハ

ードウェア、または、ソフトウェア、ファームウェアおよびハードウェアのうちの少なくとも2つの適当な組合せによって適切に実装することも可能である。このようなファームウェア実施例あるいはハードウェア実施例には、マルチ、並列および分散処理環境あるいは構成や、プログラマブルアレイロジック（PAL）およびプログラマブルロジックアレイ（PLA）、デジタル信号プロセッサ（DSP）、フィールドプログラマブルゲートアレイ（FPGA）、特定用途向け集積回路（ASIC）、大規模集積回路（LSI）、超大規模集積回路（VLSI）などのようなプログラマブル論理デバイスによって、本発明のさまざまなタイプのモジュール、回路、コントローラ、ルーチンおよびシステムを形成することが可能である。

【0076】従来のコンピュータシステムアーキテクチャは、Hans-Peter Messmer, "The Indispensable PC Hardware Book", Addison Wesley (2nd ed. 1995)、および、William Stallings, "Computer Organization and Architecture", MacMillan Publishing Co. (3rd ed. 1993)に詳細に記載されている。従来のコンピュータ（あるいは通信）ネットワーク設計は、Darren L. Spohn, "Data Network Design", McGraw-Hill, Inc. (1993)に詳細に記載されている。従来のデータ通信は、Bud Bates and Donald Gregory, "Voice and Data Communications Handbook", McGraw-Hill, Inc. (1996)、R. D. Gitlin, J. F. Hayes and S. B. Weinstein, "Data Communications Principles", Plenum Press (1992)、および、James Harry Green, "The Irwin Handbook of Telecommunications", Irwin Professional Publishing (2nd ed. 1992)に詳細に記載されている。

【0077】

【発明の効果】以上述べたごとく、本発明によれば、ユーザの秘密性を保ちながらユーザの識別を提供する、匿名性のある個人化されたウェブ閲覧を行うことが可能となる。

【図面の簡単な説明】

【図1】本発明の原理を適切に使用することにより、ネットワークのサーバサイトに代用識別子を提供してユーザが匿名的に閲覧することを可能にする中央または周辺

プロキシシステムが実現される、例示的な分散ネットワークの高水準ブロック図である。

【図2】図1の分散ネットワークにおいて、本発明の原理に従って、各ユーザサイト、中央プロキシシステムおよび複数のサーバサイトを含む例示的なサブネットワークのブロック図である。

【図3】本発明の原理によるプロキシシステムの例示的なフルスクリーンウィンドウの図である。

【図4】本発明の原理による特定サーバサイトのインタフェースの例示的なフルスクリーンウィンドウの図である。

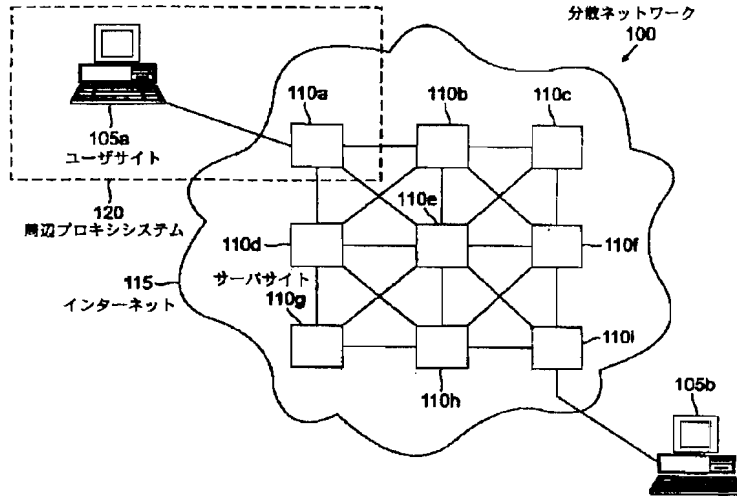
【図5】図1の分散ネットワークにおいて、本発明の原理に従って、各ユーザサイト、中央プロキシシステム、周辺プロキシシステムおよび複数のサーバサイトを含む例示的なサブネットワークのブロック図である。

【図6】図1の分散ネットワークにおいて、本発明のマークアッププロキシ実施例に従って、各ユーザサイト、中央プロキシシステムおよび複数のサーバサイトを含む例示的なサブネットワークのブロック図である。

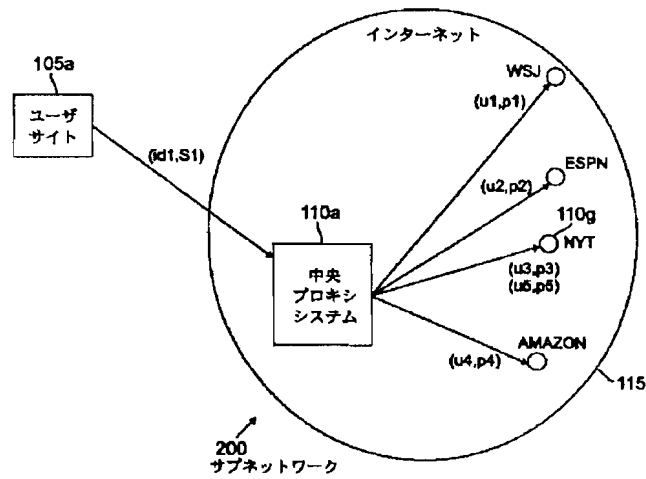
【符号の説明】

- 100 分散ネットワーク
- 105 コンピュータサイト
- 105a ユーザサイト
- 110 コンピュータサイト
- 110a 中央プロキシサイト
- 110b サーバサイト
- 110c サーバサイト
- 110g サーバサイト
- 115 インターネット
- 120 周辺プロキシシステム
- 200 サブネットワーク
- 300 ブラウザ
- 305 インタフェース（ウェブページ）
- 400 インタフェース
- 500 サブネットワーク
- 510 ローカルプロキシシステム
- 600 サブネットワーク
- 605 マークアッププログラム

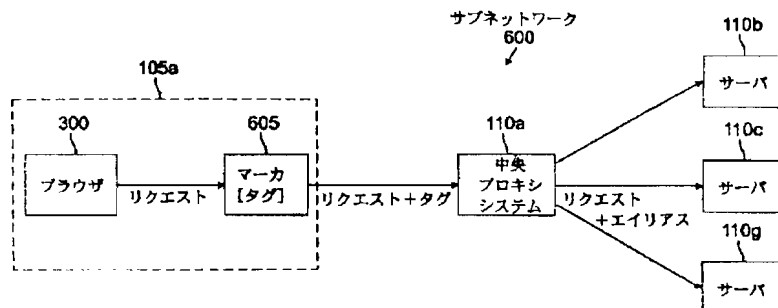
【図1】



【図2】



【図6】



【図3】

## 300 ブラウザ

Netscape: Janus User Identification

File Edit View Go Bookmarks Options Directory Window Help

Back Forward Home Reload Images Open Print Find Stop

Location:

What's New? What's Cool? Destinations Net Search People Software

## Welcome to Janus!

Janus is a system for personalized anonymous Web access.

Janus generates consistent untraceable aliases for you from the information you provide in this page. Janus neither stores this information nor passes it to any server. Consequentially, Janus does not authenticate you. You must provide the same information in future sessions to generate the same aliases.

You will see this form only once at the beginning of the session. You cannot change the input to Janus during the rest of your session, unless Janus detects that it fails to authenticate you.

The pair <user name, alias-seed> should be unique among all Janus users. You can use your E-mail address as your name to reduce chance of collision with other users. Janus will not pass your name to any server. Maximal size for user name and seeds is 1000 characters each.

Enter your user name (use your E-mail address):

Enter your secret (must contain at least 8 characters):

Verify your secret by typing it again:

Click [here](#) for more information about Janus.

ウェブ  
ページ  
305



【図4】

300

Netscape: Registration

File Edit View Go Bookmarks Options Directory Window Help

Back Forward Home Reload Images Open Print Find Stop

Netsite:

What's New? What's Cool? Destinations Net Search People Software

# The New York Tribune

## Registration

Welcome to The New York Tribune on the Web. If you're visiting us for the first time, please register now by filling out the form below. There is currently no charge for U.S. residents to subscribe to our site, but we are requiring registration, which is a one-time only process.

If you have already registered, continue to the home page. If you've registered, but are having problems entering the site, consult our help section.

Choose a Subscriber ID for The New York Tribune on the Web:

Minimum five characters

Choose a password:

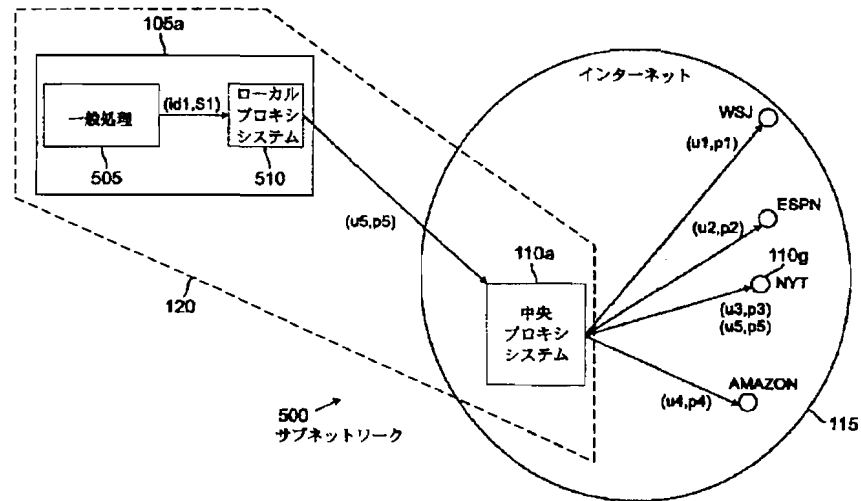
Minimum five characters

Re-enter password for confirmation:

Enter your e-mail address:

400  
インタ  
フェース

【図5】



フロントページの続き

(51)Int.Cl.<sup>6</sup>

識別記号

F I

H 0 4 L 11/20

1 0 2 A

(71)出願人 596077259  
600 Mountain Avenue,  
Murray Hill, New Je  
rsey 07974-0636 U. S. A.  
(72)発明者 フィリップ ビー. ギボンズ  
アメリカ合衆国、07090 ニュージャージ  
ー、ウェストフィールド、エンブリー コ  
ート 201

(72)発明者 ヨッシ マティアス  
アメリカ合衆国、20854 メリーランド、  
ボトマック、ロサリンダ ドライブ  
11815  
(72)発明者 アレイン ジェイ. メイヤー  
アメリカ合衆国、10025 ニューヨーク、  
ニューヨーク、ウェスト 100 ストリー  
ト 309、アパートメント 3